Experimental requirements for quantum communication complexity protocols

E. F. Galvão
Centre for Quantum Computation, Clarendon Laboratory,
Univ. of Oxford, Oxford OX1 3PU U.K.

September 6, 2000

Abstract

I present a simple two-party quantum communication complexity protocol with higher success rate than the best possible classical protocol for the same task. The quantum protocol is shown to be equivalent to a quantum non-locality test, except that it is not necessary to close the locality loophole. I derive bounds for the detector efficiency and background count rates necessary for an experimental implementation and show that they are close to what can be currently achieved using ion trap technology. I also analyze the requirements for a three-party protocol and show that they are less demanding than those for the two-party protocol. The results can be interpreted as sufficient experimental conditions for quantum non-locality tests using two or three entangled qubits.

1 Introduction

In the last few years there has been a growing interest in quantum information theory, in particular in uses of entanglement like teleportation [1], quantum cryptographic key distribution [2] and dense coding [3]. In addition to extensive theoretical work, some tasks involving manipulation of entanglement have been successfully demonstrated in practice, including teleportation [4] and quantum key distribution [5]. In this paper I discuss the feasibility of experimentally implementing another application of quantum entanglement: quantum communication complexity protocols.

The scenario of communication complexity (CC) was introduced by Yao [6], who investigated the following problem involving two separated parties (Alice and Bob). Alice receives a n-bit string x and Bob another n-bit string y, and the goal is for one of them (say Bob) to compute a certain function $f(x, y)$ with the least amount of communication between them. Of course they can always succeed by having Alice send her whole n-bit string to Bob, who then computes the function, but the idea here is to find clever ways of calculating f with less than n bits of communication. This problem is relevant in many

contexts: in electronic circuit design, for example, one wants to minimize energy use by decreasing the amount of electric signals required between the different components during a distributed computation.

Various authors have established [7, 8, 9, 10, 11] the somewhat surprising result that entanglement can be used to reduce the amount of communication necessary to calculate many functions of distributed inputs. This can be done by previously sharing entangled states between the parties, and then allowing them to do measurements on these states as part of their CC protocols. Quantum CC tries to quantify the gain obtained by using entanglement for different classes of multi-party distributed function calculations.

In this paper I present a simple two-party CC task and discuss some necessary conditions to demonstrate the quantum protocol in the laboratory. I start by describing the task itself in section 2 and its optimal classical protocol (section 2.1), followed by a more efficient quantum protocol (section 2.2). In section 2.3 I show that the efficiency of the quantum protocol relies on its equivalence to measurements that maximally violate the Clauser-Horne-Shimony-Holt (CHSH) quantum non-locality inequality. In section 2.4 I discuss some issues concerning the feasibility of implementing this protocol experimentally, and argue that ion trap technology is presently very close to achieving the necessary thresholds. In section 3 I analyse a three-party CC task discussed in [8] and show that in principle it can be demonstrated experimentally with lower detector efficiencies and higher background count rates than the two-party quantum CC protocol previously discussed. Finally in section 4 I round up with some concluding remarks.

2 A two-party communication complexity task

In [11] the authors presented a two-party CC task on which I will now elaborate, introducing a slight change in order to obtain a larger gap in efficiency between the quantum and the classical protocols. This larger difference will be important when we discuss the experimental implementation in section 2.4, as it allows for lower detector efficiencies.

The modified task can be simply stated as follows. The two parties Alice and Bob are each given a number between 0 and $2N-1$, where N is an even integer and $N \geq 4$. We can think of Alice's number x and Bob's number y as being integers modulo $2N$ lying uniformly distributed on a circle. The numbers are chosen randomly with equal probabilities, but obeying certain constraints: either

$$\text{a) } (x-y) \bmod 2N \in \{1, 2N-1\}, \tag{1}$$

in which case x and y are said to be 'neighbours', or

$$\text{b) } (x-y) \bmod 2N \in \{N-1, N+1\}, \tag{2}$$

in which case x and y are 'anti-neighbours'.

The reason for the terms 'neighbours' and 'anti-neighbours' is obvious when one looks at the two possibilities in the integers modulo $2N$ circle: in the 'neighbours' case x and y are adjacent points; in the 'anti-neighbours' case y is adjacent to the farthest point from x, which is $(x+N) \bmod 2N$. After being assigned their numbers, Alice is then allowed to communicate a single bit of information to Bob, who then has to decide whether x and y are neighbours or anti-neighbours, achieving as low an error rate as possible over many runs of the task.

This protocol represents only a slight departure from that presented in [11]. The difference here is that x and y are not allowed to coincide or to differ by $N(\bmod 2N)$, as was the case in [11]. As we will see in section 2.2, this eliminates two possibilities for which the quantum protocol does not offer advantage over the best classical one, making the quantum protocol more efficient in relation to the optimal classical counterpart.

2.1 The best possible classical protocol

In this section I describe the best possible deterministic classical protocol, and argue that it is optimal. After receiving her number x, Alice decides about which bit value to send to Bob by looking up the value of some function $g(x) = \pm 1$, as x is only data she has access to. The function $g(x)$ is also known to Bob, who upon receiving the bit from Alice learns that x lies in one of two disjunct sets, and acts in an optimal way to try to decide whether x and y are neighbours or antineighbours.

We may think of the function $g(x)$ as a colouring of the $2N$ points in the circle in either black (corresponding to $g(x) = +1$) or white ($g(x) = -1$). What Alice does is to send x's colour to Bob for him to decide which case they have. Suppose, for example, that Alice sends the bit $+1$ to Bob, corresponding to a black x. If Bob's y has two black neighbours and two white anti-neighbours, then Bob can be absolutely sure that x and y are neighbours. Of course the situation will not always be so clear-cut, forcing Bob to make informed or random guesses sometimes. One way to find the optimal deterministic classical protocol is to consider all possible $g(x)$ (=colourings) and evaluate the probability of success for Bob, using the fact that the distributions for x and y are uniform. It is a reasonable conjecture that one optimal colouring consists of one half of the circle coloured white and the other half black, which yields a success probability of

$$p_c^N = \frac{N-1}{N}. \tag{3}$$

For $N = 4$, I analysed the 16 non-equivalent possible colourings and indeed found that the optimal deterministic protocol is of the form above, having a success probability of

$$p_c^{N=4} = \frac{3}{4}. \tag{4}$$

Even though we considered only deterministic protocols, in [11] the authors showed that probabilistic protocols need not be considered for this kind of problem. This is true because any probabilistic protocol can be reduced to a deterministic one by having Alice and Bob share random numbers before they are assigned x and y. As a result, for $N = 4$ the best possible classical protocol is the one described above, achieving a success probability of $p_c = 3/4$.

2.2 The quantum protocol

Here I describe a quantum protocol which accomplishes the task with a larger success probability than the optimal classical protocol described above. The motivation for this protocol comes from the visualization of x and y on the $\bmod 2N$ circle, where they lie separated by an angle which is either π/N or $(N-1)\pi/N$. It is a well known fact that local rotation followed by measurements on maximally entangled states yield strong correlations which are not allowed classically [12, 13, 14], and which will be used in the protocol.

Before they are given their numbers, Alice and Bob meet and share a singlet state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|+\rangle_A |-\rangle_B - |-\rangle_A |+\rangle_B \right). \tag{5}$$

For simplicity of description, we will assume that $|\psi\rangle$ was shared in the form of an entangled pair of spin-1/2 particles. Upon receiving her number, Alice measures the spin on her particle along the axis defined by the angle $\theta = \pi x/N$ to the z axis on the xy plane, and sends the result (± 1) to Bob. He measures the spin on his particle along the axis defined by the angle $\phi = \pi y/N$ to the z axis on the xy plane, also obtaining a result ± 1. It does not matter whether he does this before or after receiving Alice's message. Bob's decision is made in a simple way: if the two measurement results are the same he guesses that x and y are neighbours, otherwise that they are anti-neighbours.

Let us now evaluate the probability of error if Bob and Alice adopt this protocol. For the singlet state one can easily show that

$$p(\text{same} \mid \theta, \phi) = \frac{1}{2}(1 - \cos(\theta - \phi)) \tag{6}$$

$$p(\text{opposite} \mid \theta, \phi) = \frac{1}{2}(1 + \cos(\theta - \phi)), \tag{7}$$

where $p(\text{same}|\ \theta, \phi)$ is the probability that their outcomes are the same and $p(\text{opposite}|\ \theta, \phi)$ is the probability that their outcomes are opposite. In the 'neighbours' case we have $|\theta - \phi| = \pi/N$ and hence

$$p_{\text{success}}(\text{neighbours}) = p(\text{opposite} \mid \theta, \phi) = \frac{1}{2}(1 + \cos(\pi/N)).$$

In the 'anti-neighbours' case we have either $|\theta - \phi| = \pi + \pi/N$ or $|\theta - \phi| = \pi - \pi/N$, from which we find

$$p_{\text{success}}(\text{anti-neighbours}) = p(\text{opposite} \mid \theta, \phi) = \frac{1}{2}(1 + \cos(\pi/N)).$$

In any case, we see that this protocol is successful with a probability

$$p_q = \frac{1}{2}(1 + \cos(\pi/N)), \tag{8}$$

which is always larger than the conjectured classical success probability given by eq. (3), and definitely larger than the best classical protocol for $N = 4$, whose success probability is limited to $p_c = 3/4$ [compare with $p_q = 1/2(1+\cos(\pi/4)) \simeq 0.8536$].

Unlike the classical protocol, the quantum version has a probability of success which is independent of the probability distribution for x and y. This, however, should not be considered a substantial advantage for the quantum protocol, as a randomized classical protocol can be used to obtain $p_c = (N-1)/N$ even for non-uniform distributions of x and y. This can be done by having Alice and Bob choose different optimal colourings for each run, according to previously shared random numbers.

In the protocol described above the singlet state (5) is measured along directions that differ by either π/N or $(N-1)\pi/N$. This is in contrast with the quantum protocol for the task presented in [11], whose measurements include those but also measuments along the same axis. Since the quantum and classical correlations are equal (and maximal) for measurements along the same axis, we obtain a larger gap between the classical and quantum efficiencies by eliminating this possibility, which we did by redefining the task suitably.

2.3 Quantum protocol as a Bell inequality test

The quantum protocol described above is clearly inspired by the CHSH inequality presented in [13], which establishes bounds for classical correlations between simultaneous measurements on maximally entangled states. In fact, we will see that there is a simple interpretation of the quantum protocol in terms of Bell-type quantum non-locality tests.

In [14] an inequality was derived for classical correlations between measurements with two possible outcomes (denoted by $+$ or $-$), arising from experiments with $N/2$ different setups at Alice's laboratory and $N/2$ at Bob's. We write $p^e(a_i, b_j)$ to denote the probability of obtaining two equal outcomes ($++$ or $--$) with setups a_i at Alice and b_j at Bob, and similarly $p^d(a_i, b_j)$ for different outcomes ($+-$ or $-+$). For $N = 4$ we have the following inequality [14]:

$$p^d(a_1, b_1) + p^d(a_2, b_1) + p^d(a_2, b_2) + p^e(a_1, b_2) \leq 3, \tag{9}$$

which must be obeyed by *any* local theory. This inequality is saturated by a simple 'classical spin' local model described in [12, 14, 15]. It is easy to see

that quantum mechanics violates inequality (9) for measurements on the singlet state (5). Choosing the angles of measurement to be $a_1 = 0, a_2 = \pi/2, b_1 = \pi/4, b_2 = 3\pi/4$ we obtain maximal violation of inequality (9):

$$p_q^d(a_1, b_1) = p_q^d(a_2, b_1) = p_q^d(a_2, b_2) = p_q^e(a_1, b_2) = \frac{1}{2}\left(1 + \frac{\sqrt{2}}{2}\right) \tag{10}$$

$$\Rightarrow p_q^d(a_1, b_1) + p_q^d(a_2, b_1) + p_q^d(a_2, b_2) + p_q^e(a_1, b_2) = 2 + \sqrt{2} > 3. \tag{11}$$

We see that the quantum mechanics predictions violate the inequality, and therefore are impossible to be accounted for by any local theory. The same setup also maximally violates the CHSH inequality, as discussed in [13]; in fact Hardy has shown [14] that the CHSH inequality can be obtained from (9).

It is interesting to note that there is an exact correspondence between the measurements that maximally violate inequality (9) and the quantum protocol for $N = 4$ described above. In both cases the two parties do measurements on a singlet state along co-planar directions separated by two possible angles: $\pi/4$ or $3\pi/4$ radians. In the quantum protocol we want to maximize

$$p_q = p_{success}(\text{neighbours}) + p_{success}(\text{anti-neighbours}).$$

The inequality test described above corresponds to a similar situation. Quantum mechanics predicts $p_q^d(a_1, b_1) = p_q^d(a_2, b_1) = p_q^d(a_2, b_2) = p_{success}(\text{neighbours})$ and $p_q^e(a_1, b_2) = p_{success}(\text{anti-neighbours})$, and we maximize $3p_{success}(\text{neighbours}) + p_{success}(\text{anti-neighbours})$ in order to violate the inequality by the greatest amount. As $p_{success}(\text{neighbours}) = p_{success}(\text{anti-neighbours})$, the maximization of the violation of inequality (11) also maximizes the probability of success p_q. Curiously, the 'classical spin' model used to saturate the inequality turns out to be equivalent to the best classical protocol for the task, that is, it can be used as an alternative to the optimal classical protocol described in section 2.1.

The key difference between the measurements used in the quantum protocol and the CHSH inequality test is the number of possible setups at Alice and Bob. For the CHSH inequality violation we consider two setups at Alice and two at Bob, whereas in the quantum protocol Alice and Bob need to use one of four possible setups. The 'promise' that x and y are either neighbours or antineighbours guarantees that for each run the measurements at Alice and Bob will be done along angles that differ either by $\pi/4$ or $3\pi/4$ radians, like the CHSH test. But unlike it, the quantum protocol relies on Alice using one of four possible setups; she cannot communicate this to Bob with a single bit. Instead, she communicates the result of the measurement to Bob, who can then use the stronger-than-classical correlations between the measurements to obtain success with a high probability.

2.4 Experimental implementation

The quantum CC protocol of section 2.2 with $N = 4$ is arguably the simplest to implement in the laboratory. There is a clear-cut criterion for experimental success: if after a large number of runs the success rate is found to be larger than 3/4 then entanglement-enhanced CC will have been demonstrated. In [8] a similar CC task was presented which has the same classical and quantum error rates as the one here, and which therefore needs an equivalent detector efficiency to be implemented (as we will see below). The advantages of the present task is that it is simpler to describe and easier to interpret in terms of Bell-type inequalities, as discussed in the previous section.

It is important to point out that in order to experimentally implement this quantum CC protocol it is *not* necessary to have space-like separated measurements at Alice and Bob. Unlike Bell inequality tests, here the two parties are *required* to communicate before finishing the task. All that is needed for a successful experiment is to implement the quantum protocol in such a way as to obtain a success rate which is higher than that of the highest classical protocol. Once this is done, one might correctly argue that, from a fundamental point of view, local hidden-variable theories cannot be ruled out as the responsible for the better performance of the quantum protocol. From a practical point of view, however, after a large enough number of runs this would be an undeniable demonstration of entanglement-assisted communication. The question of whether local hidden variable theory or quantum mechanics is the correct theory to explain the enhancement becomes immaterial if we are only concerned about establishing an experimental evidence for the effect.

Given the equivalence of the protocol with a CHSH inequality test, the experimental problems to be taken into account are those of a CHSH test, except that we do not need to close the locality loophole. With this in mind, we can calculate necessary bounds for the detector efficiency and background levels.

For the quantum protocol to beat the best classical one for $N = 4$ we need a success rate higher than $p_c = 3/4$. First I will analyse the case of no background detections, and detectors that either obtain the correct result or fail to register the event [16]. With a finite detector efficiency $\eta < 1$, Alice and Bob must agree on a procedure for the case when their detectors fail. They are not allowed to communicate the failure, as this would consist of further bits of communication between the parties, and the communication allowed is restricted to one bit. The most effective way is for Alice to proceed with the best classical protocol in case her detector fails, and for Bob to do the same when his detector fails. Whenever both detectors fail, Alice and Bob will obtain the best classical sucess rate. In the case of a single detector failure, Bob's guess will still be correct with $p = 1/2$. Assuming independent errors at the two detectors, we can calculate the minimum detector efficiency needed:

$$\eta^2 p_q + (1-\eta)^2 p_c + \eta(1-\eta)\frac{1}{2} + (1-\eta)\eta\frac{1}{2} > p_c$$
$$\Rightarrow \eta > \frac{2p_c - 1}{p_q + p_c - 1}.$$

For the case $N = 4$ that we analysed, we have $p_q = 1/2 + \sqrt{2}/4$ and $p_c = 3/4$, which results in a minimum necessary detector efficiency

$$\eta_{\min} = 2(\sqrt{2} - 1) \simeq 0.828,$$

which is also the minimum detector efficiency necessary for a loophole-free CHSH inequality test [17]. A similar analysis can be done for general N, and it turns out that the minimum detector efficiency required increases with increasing N, making the $N = 4$ case the most interesting for an experimental test.

We can include background detections in the analysis by introducing a factor μ, defined such that $(1 - \mu)$ is the fraction of detections that are due to background photons. We assume completely random background detections, yielding each measurement outcome with probability $p = 1/2$. Note that imperfections in the state preparation procedure can also be incorporated in the model through the parameter μ. Each run of the experiment can then be classified into one of three categories:

1) Alice and Bob measure their parts of the EPR pair accurately with probability $\eta^2\mu^2$, in which case they apply the quantum protocol and succeed with probability p_q.

2) Both their detectors fail to detect anything, which will happen in a fraction $(1 - \eta)^2$ of the runs. In this situation they will both use the classical protocol with a probability of success p_c.

3) In all the other situations Bob will use either the quantum or the classical protocol, depending on whether he detects a photon or not. However, due to either background or lack of detection at Alice's side his guesses will be random, yielding a success rate of only $1/2$.

Taking all this into account, the condition for a higher-than-classical success rate is:

$$\eta^2\mu^2 p_q + (1-\eta)^2 p_c + (1 - \eta^2\mu^2 - (1-\eta)^2)\frac{1}{2} > p_c. \tag{12}$$

With p_c and p_q from our task with $N = 4$, this is equivalent to

$$\mu > \frac{1}{2\eta}\sqrt{2\sqrt{2}\eta(2-\eta)}. \tag{13}$$

In particular, for perfect detectors ($\eta = 1$), we need $\mu > 2^{-1/4} \simeq 0.841$. In Figure 1 we represent the region in the $\eta - \mu$ parameter space that guarantees a higher-than-classical success rate.

The favourable $\eta - \mu$ region represents exactly the same conditions necessary for a violation of the CHSH inequality (as can be gathered from [19], for example). This is not a surprise, given the equivalence between the quantum protocol and a CHSH test pointed out in section 2.3. More generally, whenever we have a quantum CC protocol outperforming the optimal classical protocol for a given CC task, the measurements involved in the quantum protocol can be re-interpreted in terms of a non-locality proof. This is the case at least for tasks allowing only one round of communication between the parties, as the one presented above and the one we will analyse in the next section. For this class of CC tasks, it is always possible to carry out the protocol in such a way as to enforce that all measurements on entangled states be performed in space-like separated regions; if despite this, the CC task is performed with higher than classical efficiency, it must be because of stronger-than-classical correlations among the results of the measurements of the quantum protocol.

Maximally entangled pairs of photons can be generated with high fidelity and measured with precision, which guarantees the equivalent of a very high μ. However, detector efficiencies η are still short of those necessary. Ion traps techniques, on the other hand, can reach high η and μ [18]. This makes ion traps a natural choice for the experimental demonstration of the simple quantum communication complexity task presented here.

3 A three-party task

In this section I will discuss the three-party communication complexity (CC) task described in [8], finding the necessary experimental requirements for the demonstration of a quantum protocol for it. The enhancement in performance with relation to the best classical protocol arises from measurements on a tripartite Greeberger-Horne-Zeilinger (GHZ) state [20, 21, 22]

$$|GHZ\rangle = \frac{1}{\sqrt{3}}(|0_A 0_B 0_C\rangle + |1_A 1_B 1_C\rangle).$$

The state preparation and measurement tend to be much harder to perform experimentally than for the two-party protocol described in section 2.2. In principle, however, we will see that the three-party quantum protocol requires lower detector efficiencies and tolerates higher background count rates than the two-party protocol discussed above.

The CC task is defined as follows [8]. Alice, Bob and Claire receive respectively the numbers x, y and $z \in U = \{0, 1, 2, 3\}$, and these are guaranteed to satisfy

$$(x + y + z) \bmod 2 = 0. \tag{14}$$

The goal is for Alice to learn the value of the function

$$f(x, y, z) = \frac{1}{2}[(x + y + z) \bmod 4]$$

(which can be either 0 or 1), after receiving a single bit of communication from each Bob and Claire. We assume an uniform probability distribution for x, y and z, subject to satisfying eq. (14).

There is a quantum protocol which succeeds with probability $p_q = 1$ (see [8]). It is inspired by the GHZ non-locality proof of [20, 21, 22].

The best classical protocol, however, succeeds only with a lower probability p_c. In order to calculate it, we first note that for each possible x all four possibilities for y and z are allowed by condition (14), provided they are properly paired. This means that by knowing x, Alice cannot infer any information about the values of Bob's y and Claire's z, as they are all equally likely candidates. Therefore the best possible procedure for Bob will be to agree beforehand on the encoding scheme for his message, so that his bit of communication informs Alice that y lies in one of two disjunct sets, each containing two possible y values. The same holds for Claire and her one-bit message about z.

The task involves the assumption that all x, y and z values satisfying (14) will be chosen with equal probabilities. As all 16 possible combinations of y and z appear the same number of times in the full list of possibilities, this means that the choice of two-element disjunct sets for the encoding is not important, all yielding the same probability of success p_c. We can calculate p_c by choosing any such encoding for Bob and Claire, and averaging over the probability of success for all possible x, y and z. This results in the highest classical success probability

$$p_c = 3/4.$$

If we are to implement the quantum protocol in the laboratory, then we have to account for imperfect detectors and state preparation. The analysis is similar to that presented in section 2.4, with the difference that here we have three detectors instead of two. We define the background rate $(1 - \mu)$ as the fraction of events detected at each detector which are due to noise; we assume the worst-case scenario of completely random detection outcomes from these events. The single detector efficiency η is the fraction of all events that result in a detector firing. Whenever we detect a signal from the three detectors (which will happen with probability $\eta^3\mu^3$), the quantum protocol works with probability $p_q = 1$. If Alice's detectors does not fire, she will rely on the possibility of Bob's and Claire's detectors not firing either, and on them using the optimal classical protocol; this will happen with probability $(1 - \eta)^3$ and result in a probability of success $p_c = 3/4$. In all other cases, Alice will only be able to make random guesses, succeeding with probability $1/2$. Assuming independent errors at each detector, for a higher-than-classical probability of success we need

$$\eta^3\mu^3 p_q + (1-\eta)^3 p_c + [1-\eta^3\mu^3-(1-\eta)^3]\frac{1}{2} > p_c. \tag{15}$$

Substituting $p_c = 3/4$ and $p_q = 1$ into the inequality above, we obtain

$$\mu > \frac{1}{2\eta}(4\eta^3 - 12\eta^2 + 12\eta)^{1/3}. \tag{16}$$

This inequality gives us the region in the $\mu - \eta$ parameter space that allows for a successful experimental test of the quantum protocol. For perfect detectors ($\eta = 1$) we need

$$\mu > 2^{-1/3} \simeq 0.794,$$

whereas for zero background and perfect state preparation and measurement ($\mu = 1$), it is sufficient to have

$$\eta > \frac{1}{2}(\sqrt{21} - 3) \simeq 0.791.$$

Note that these are less demanding requirements than those necessary for the bipartite quantum CC protocol [see eqs. (12) and (13)]. This is related to the fact that quantum non-locality tests for multiparticle states can be done with lower detector efficiencies than for the two-particle case [23, 24, 25]. Given the possibility of interpreting the higher-than-classical performance of the quantum protocol in terms of a quantum non-locality test (as was pointed out at the end of section 2.4), we can view requirement (16) as a sufficient condition for testing quantum non-locality for three maximally entangled particles. Besides limited detector efficiency, here we consider also limited visibility (due to background counts), a situation which has not been considered before. However, the bound (16) is not strict; the simplest way to see this is by noting that with $\mu = 1$, a GHZ test can be performed whenever $\eta > .75$ if we assume independent errors [24].

4 Conclusion

I have presented a simple two-party communication complexity task which can be implemented with a higher-than-classical success rate using quantum entanglement. The efficiency of the quantum protocol was shown to be linked to its equivalence to measurements that maximally violate the CHSH inequality. In order to obtain a higher success rate than classically possible, it is sufficient to have detector efficiencies and background count rates compatible with those necessary for a CHSH test (see Fig. 1).

I have also analysed the experimental requirements for a three-party quantum communication complexity protocol presented in [8] and have shown that the requirements are less demanding than for the two-party protocol discussed. At least for the two-party protocol, the experimental requirements are within reach of currently available ion trap technology, indicating the feasibility of demonstrating quantum communication complexity protocols experimentally in the near future.

Some relations were pointed out between quantum non-locality proofs and quantum communication complexity protocols. In particular, I have shown that sufficient conditions for violation of quantum non-locality inequalities can be derived from the analysis of quantum communication complexity protocols of two or more parties.

5 Acknowledgments

I would like to thank Jan-Åke Larsson for pointing out a mistake in an earlier version of this paper and Lucien Hardy for valuable discussions. I acknowledge support from the U.K. Overseas Research Studentships scheme and from the Brazilian agency Coordenação de Aperfeiçoamento de Pessoal de Nivel Superior (CAPES).

References

[1] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).

[2] C. H. Bennett and G. Brassard "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computer Systems and Signal Processing, Bangalore, India, December 1984, pp 175-179; D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996); *erratum* **80**, 2022 (1998); D. Mayers, LANL e-print quant-ph/9802025; H. -K. Lo, H. F. Chau, LANL e-print quant-ph/9803006.

[3] C. H. Bennett, S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[4] D. Bouwmeester *et al.*, Nature (London) **390**, 575 (1997); D. Boschi *et al.,* Phys.Rev.Lett. **80**, 1121 (1998); A. Furusawa *et al.*, Science **282**, 706 (1998).

[5] C. H. Bennett et al.,Lecture Notes in Computer Science **473**, 253 (1990); C. H. Bennet et al., J. Cryptology **5**, 3 (1992); B. C. Jacobs, J. D. Franson, Opt. Lett. **21**, 1854 (1996).

[6] A. C. Yao, in Proc.11th Ann. ACM Symp. on Theory of Computing (1979), pp. 209-213.

[7] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

[8] H. Buhrman, R. Cleve and W. van Dam, Los Alamos electronic preprint quant-ph/9705033.

[9] H. Buhrman *et al.*, Phys. Rev. A **60**, 2737 (1999).

[10] R. Raz, Proc. 31st Ann. ACM Symp. on Theory of Computing (1999), pp. 358-367 .

[11] L. Hardy and W. van Dam, Phys. Rev. A **59**, 2635 (1999).

[12] J. S. Bell, Physics **1**, 195 (1965).

[13] J. F. Clauser *et al.*, Phys. Rev. Lett. **23**, 880 (1969).

[14] L. Hardy, Phys. Lett. A **161**, 21 (1991).

[15] A. Peres, *Quantum theory: concepts and methods* (Kluwer Academic, Dordrecht 1993), chapter 5.

[16] This calculation was also done independently by W. van Dam, *Non-locality & Communication Complexity*, PhD Thesis, Department of Physics, University of Oxford (1999).

[17] A. Garg, N. D. Mermin, Phys. Rev. D **35**, 3831 (1987).

[18] Q. A. Turchette *et al.*, Phys. Rev. Lett. **81**, 3631 (1998); C. Monroe *et al.*, 'Scalable entanglement of trapped ions', to appear in Proc. 17th Int. Conf. on Atomic Physics; D. Wineland, private communication (2000).

[19] J.-Å. Larsson, Phys. Lett. A **256**, 245 (1999).

[20] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989).

[21] N. D. Mermin, Phys. Today **43** (6), 9 (1990).

[22] D. M. Greenberber, M. A. Horne, A. Shimony, and a. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[23] J.-Å. Larsson, Phys. Rev. A **57**, 3304(1998).

[24] J.-Å. Larsson, Phys. Rev. A **57**, R3145 (1998).

[25] J.-Å. Larsson and J. Semitecolos, Los Alamos electronic preprint quant-ph/0006022.

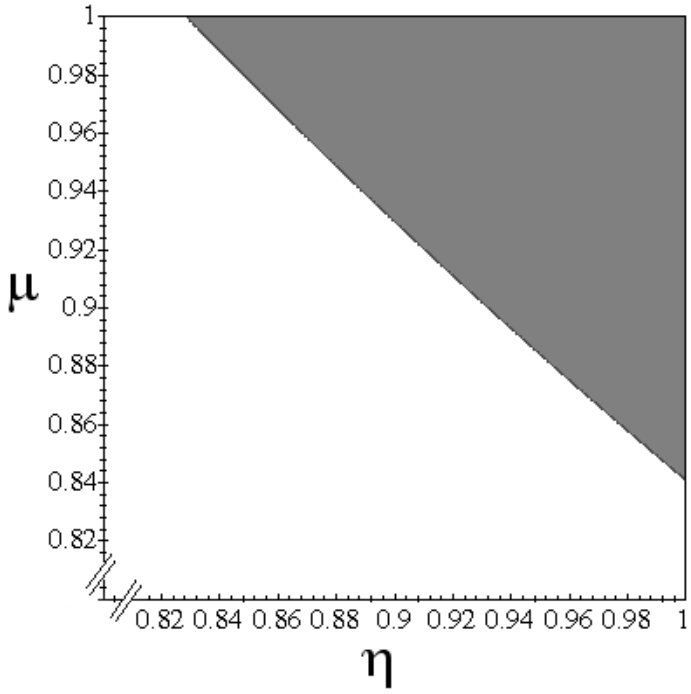

Figure 1: The shaded area indicates the region where the background level $(1-\mu)$ and detector efficiency η allow for a two-party quantum communication complexity protocol which is more efficient than any classical one for the same task. The area corresponds to that given by inequality (13).